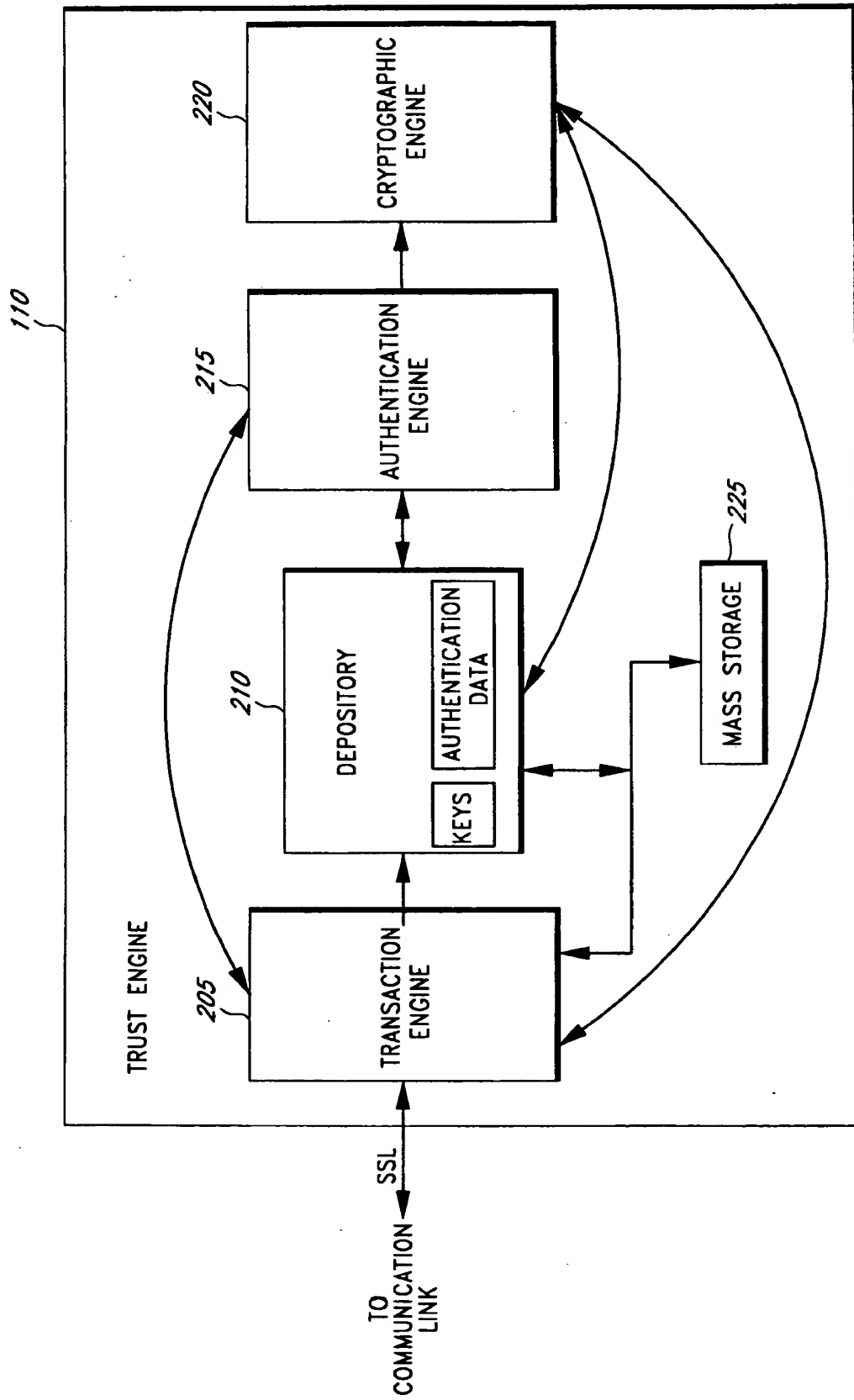


FIG. 1

**FIG. 2**

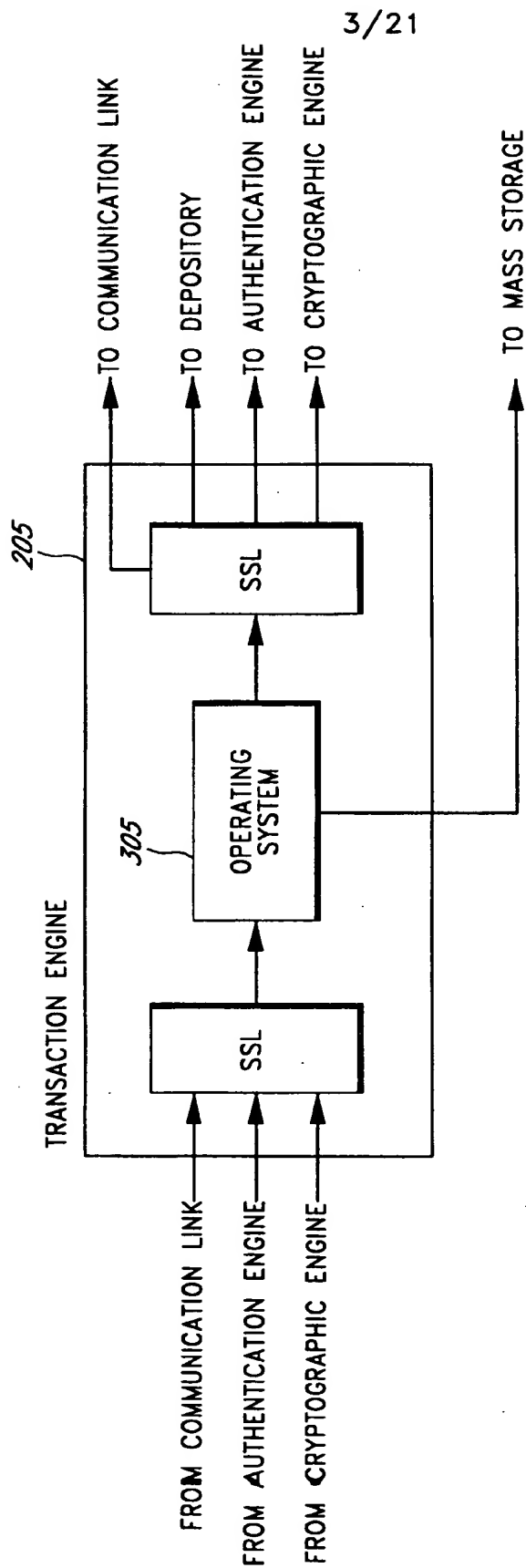
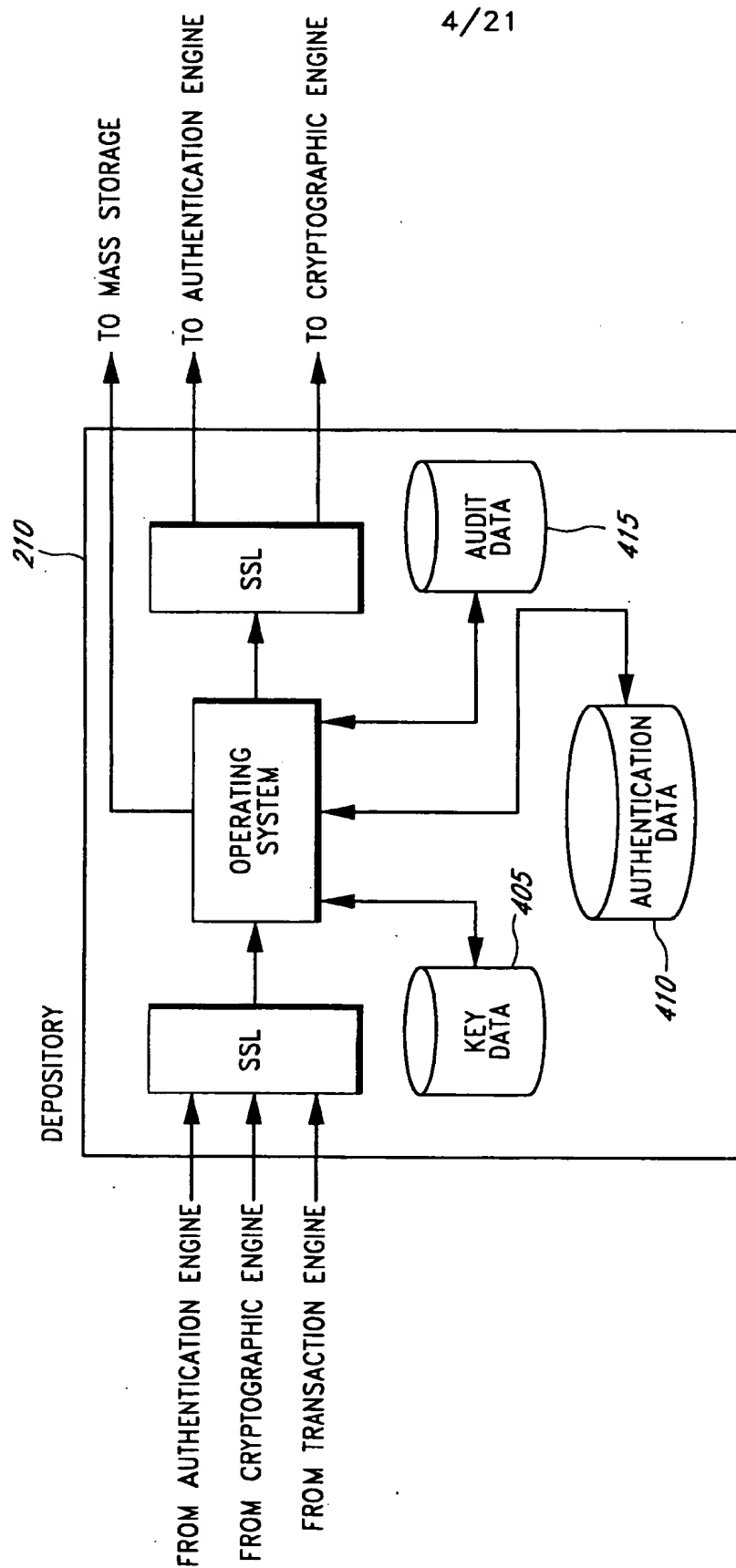


FIG. 3



4/21

FIG. 4

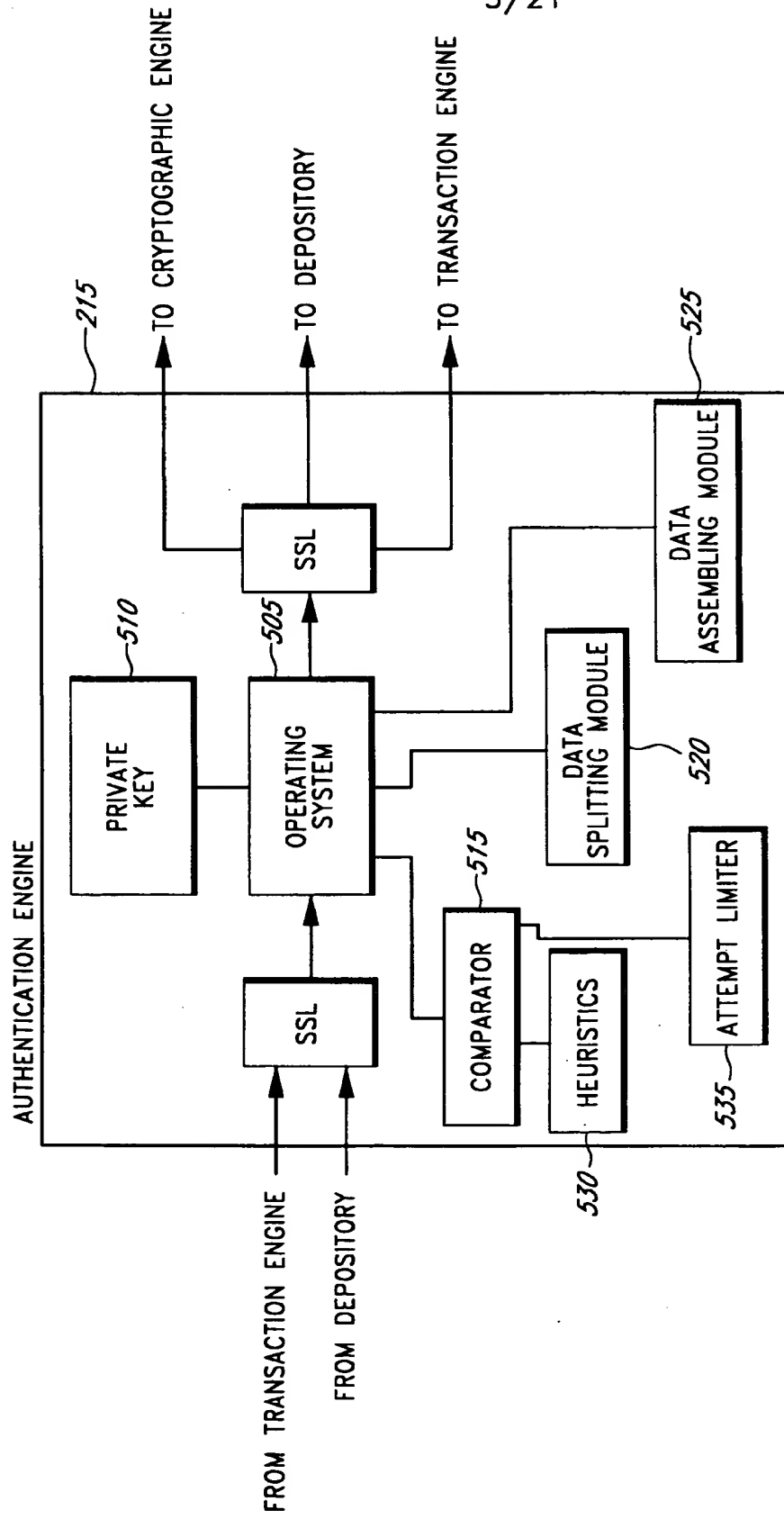
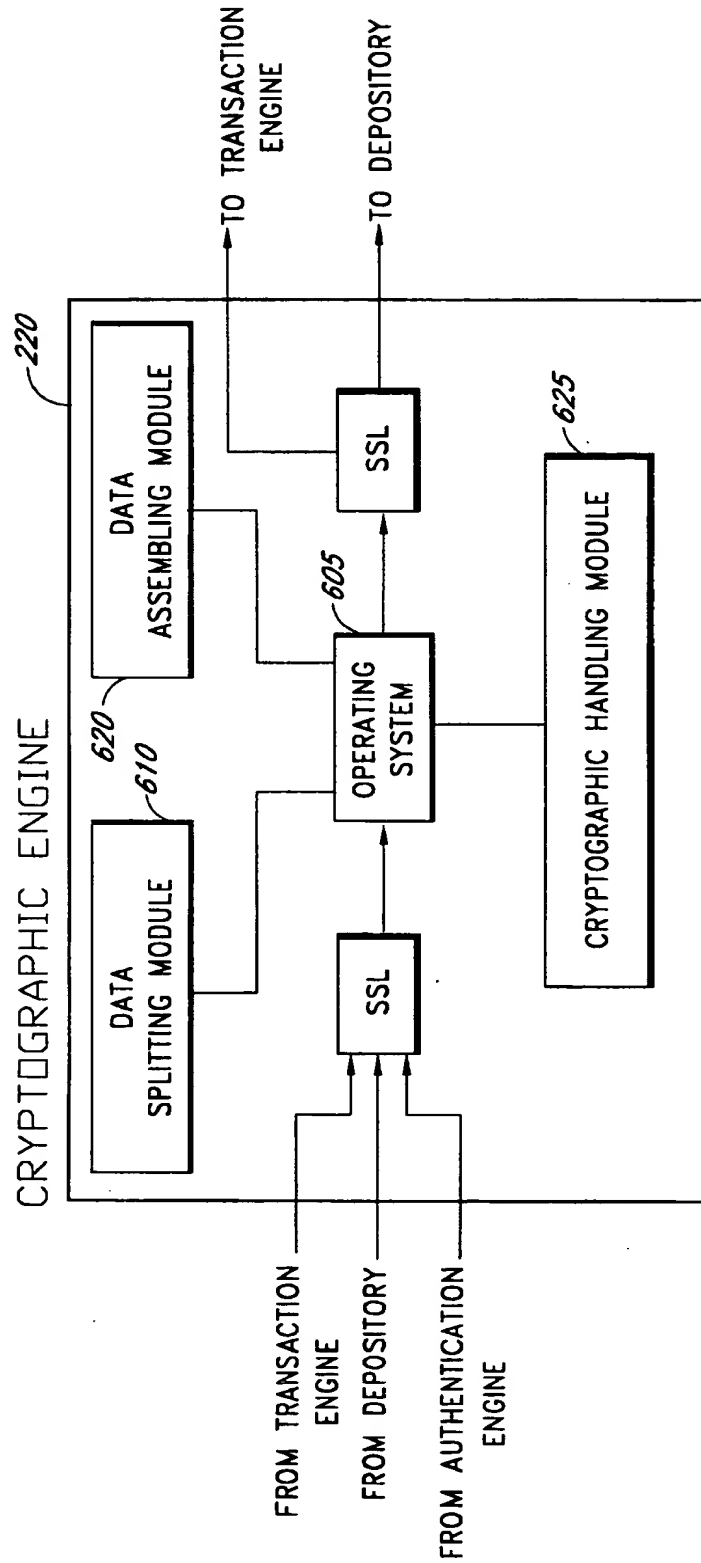


FIG. 5

**FIG. 6**

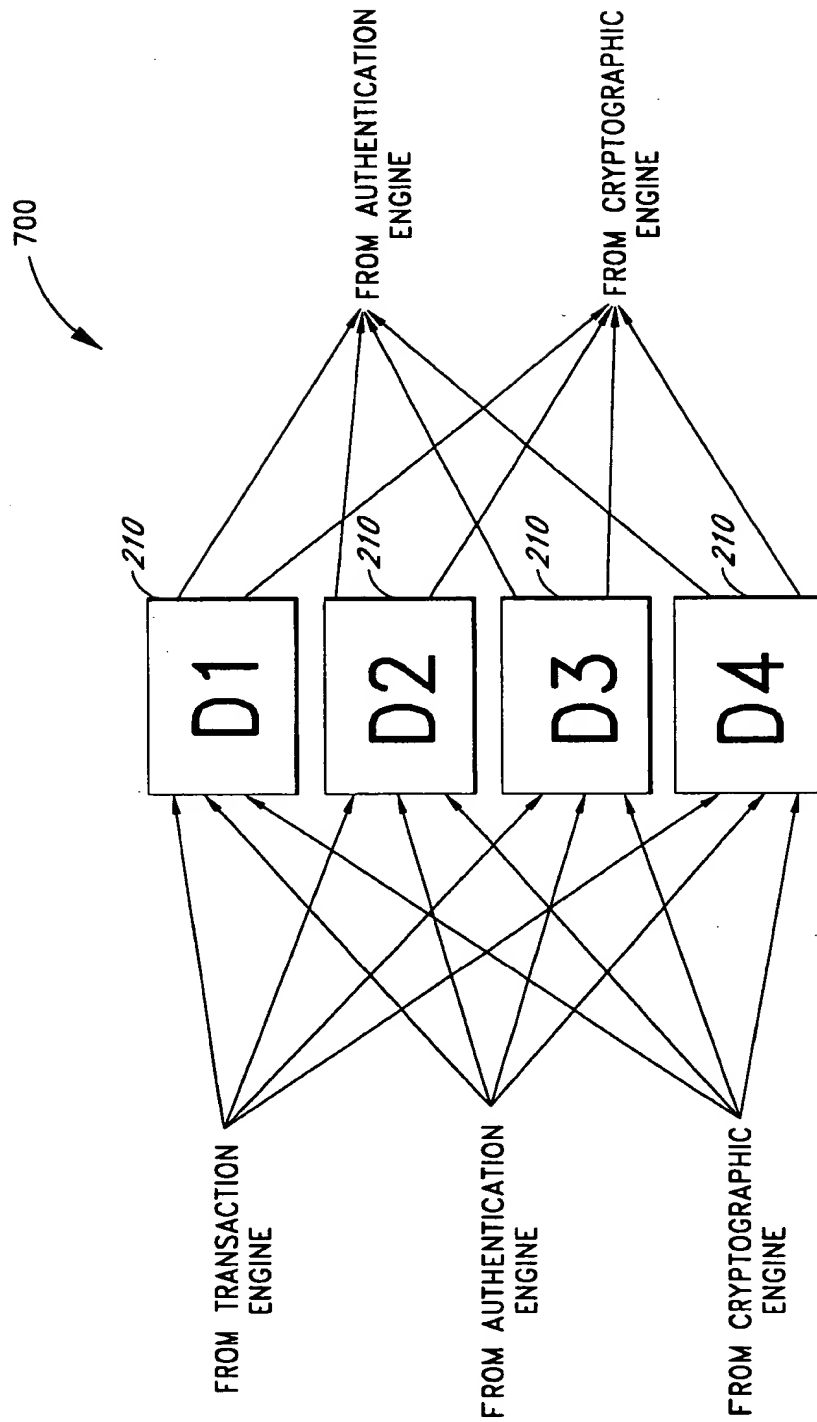
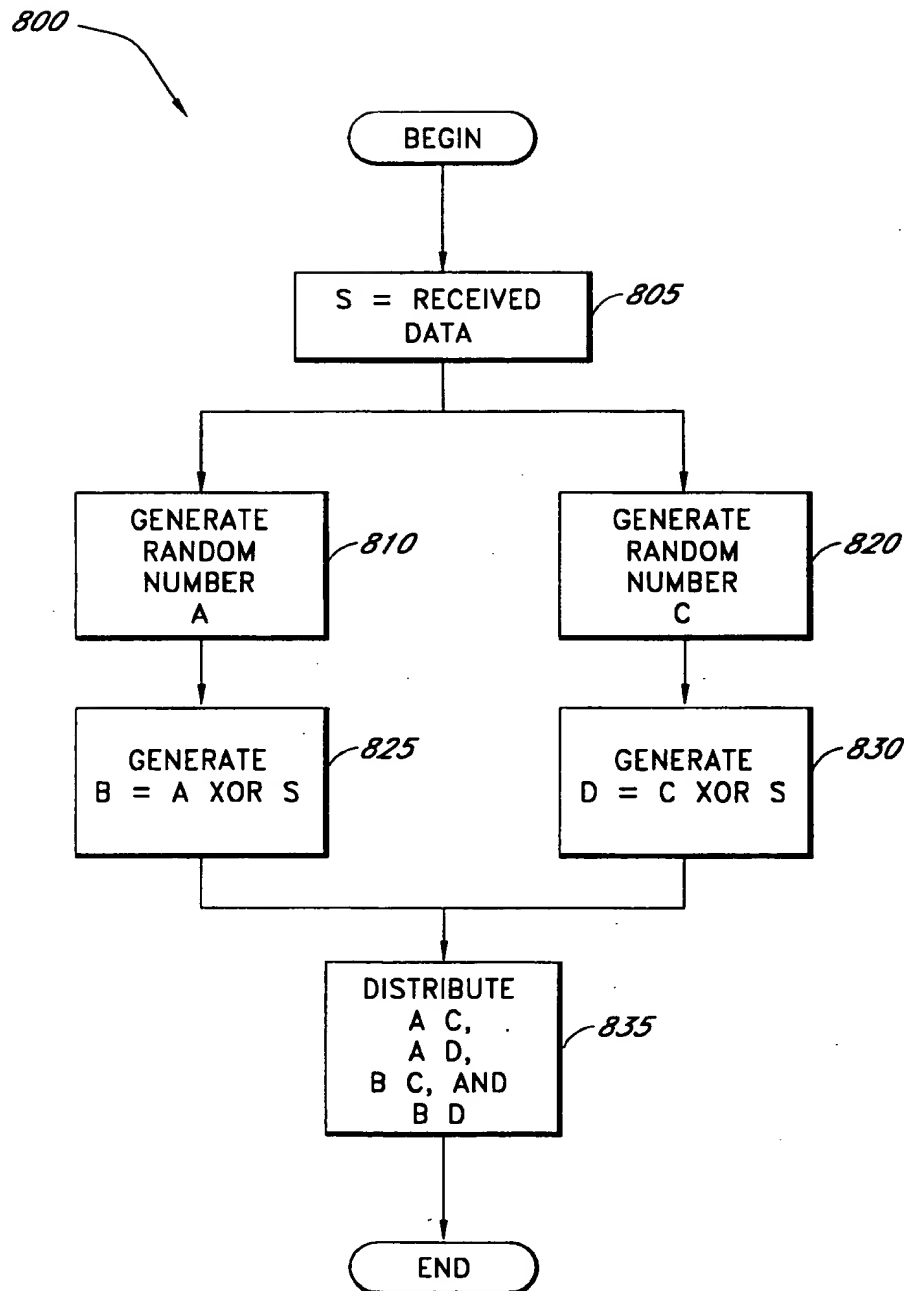


FIG. 7

**FIG. 8**

900

| ENROLLMENT DATA FLOW | | | |
|------------------------------------|------------------------------|------|--|
| SEND | RECEIVE | SSL | ACTION |
| 905 USER | TRANSACTION ENGINE (TE) | 1/2 | TRANSMIT ENROLLMENT AUTHENTICATION DATA (B) AND THE USER ID (UID) ENCRYPTED WITH THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS (PUB_AE(UID,B)) |
| 915 TE | AE | FULL | FORWARD TRANSMISSION |
| 920 | | | AE DECRYPTS AND SPLITS FORWARDED DATA |
| 925 AE | THE Xth DEPOSITORY (DX) | FULL | STORE RESPECTIVE PORTION OF DATA |
| WHEN DIGITAL CERTIFICATE REQUESTED | | | |
| 930 AE | CRYPTOGRAPHIC ENGINE (CE) | FULL | REQUEST KEY GENERATION |
| 935 | | | CE GENERATES AND SPLITS KEY |
| 945 CE | TE | FULL | TRANSMIT REQUEST FOR DIGITAL CERTIFICATE |
| 950 TE | CERTIFICATION AUTHORITY (CA) | 1/2 | TRANSMIT REQUEST |
| 955 CA | TE | 1/2 | TRANSMIT DIGITAL CERTIFICATE |
| 960 TE | USER | 1/2 | TRANSMIT DIGITAL CERTIFICATE |
| TE | MS | FULL | STORE DIGITAL CERTIFICATE |
| 965 TE | DX | FULL | STORE RESPECTIVE PORTION OF KEY |

FIG. 9A

10/21

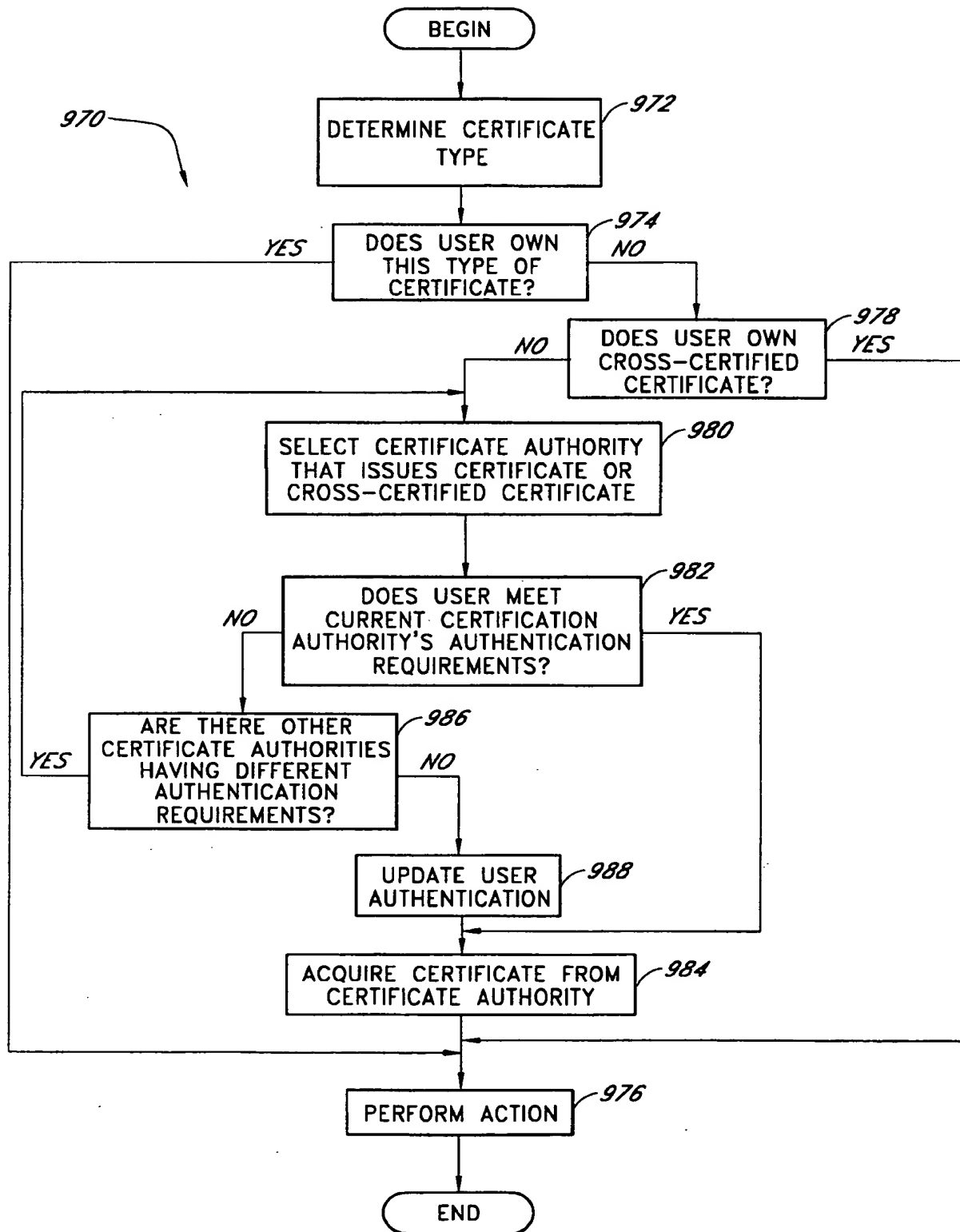


FIG. 9B

AUTHENTICATION DATA FLOW

| | SEND | RECEIVE | SSL | ACTION |
|------|--------|-------------------------|------|--|
| 1005 | USER | VENDOR | 1/2 | TRANSACTION OCCURS, SUCH AS SELECTING PURCHASE |
| 1010 | VENDOR | USER | 1/2 | TRANSMIT TRANSACTION ID (TID) AND AUTHENTICATION REQUEST (AR) |
| | | | | AUTHENTICATION DATA (B') IS GATHERED FROM USER |
| 1015 | USER | TE | 1/2 | TRANSMIT TID AND B' WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE), AS (PUB_AE(TID, B')) |
| 1020 | TE | AE | FULL | FORWARD TRANSMISSION |
| | | | | ENROLLMENT AUTHENTICATION DATA (B) IS REQUESTED AND GATHERED |
| 1025 | VENDOR | TRANSACTION ENGINE (TE) | FULL | TRANSMITS TID, AR |
| 1030 | TE | MASS STORAGE(MS) | FULL | CREATE RECORD IN DATABASE |
| 1035 | TE | THE Xth DEPOSITORY(DX) | FULL | UID, TID |
| 1040 | DX | AE | FULL | TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX) AS (PUB_AE(TID, BX)) |
| 1045 | | | | AE ASSEMBLES B AND COMPARES TO B' |
| 1050 | AE | TE | FULL | TID, THE FILLED IN AR |
| | TE | VENDOR | FULL | TID, YES/NO |
| 1055 | TE | USER | 1/2 | TID, CONFIRMATION MESSAGE |

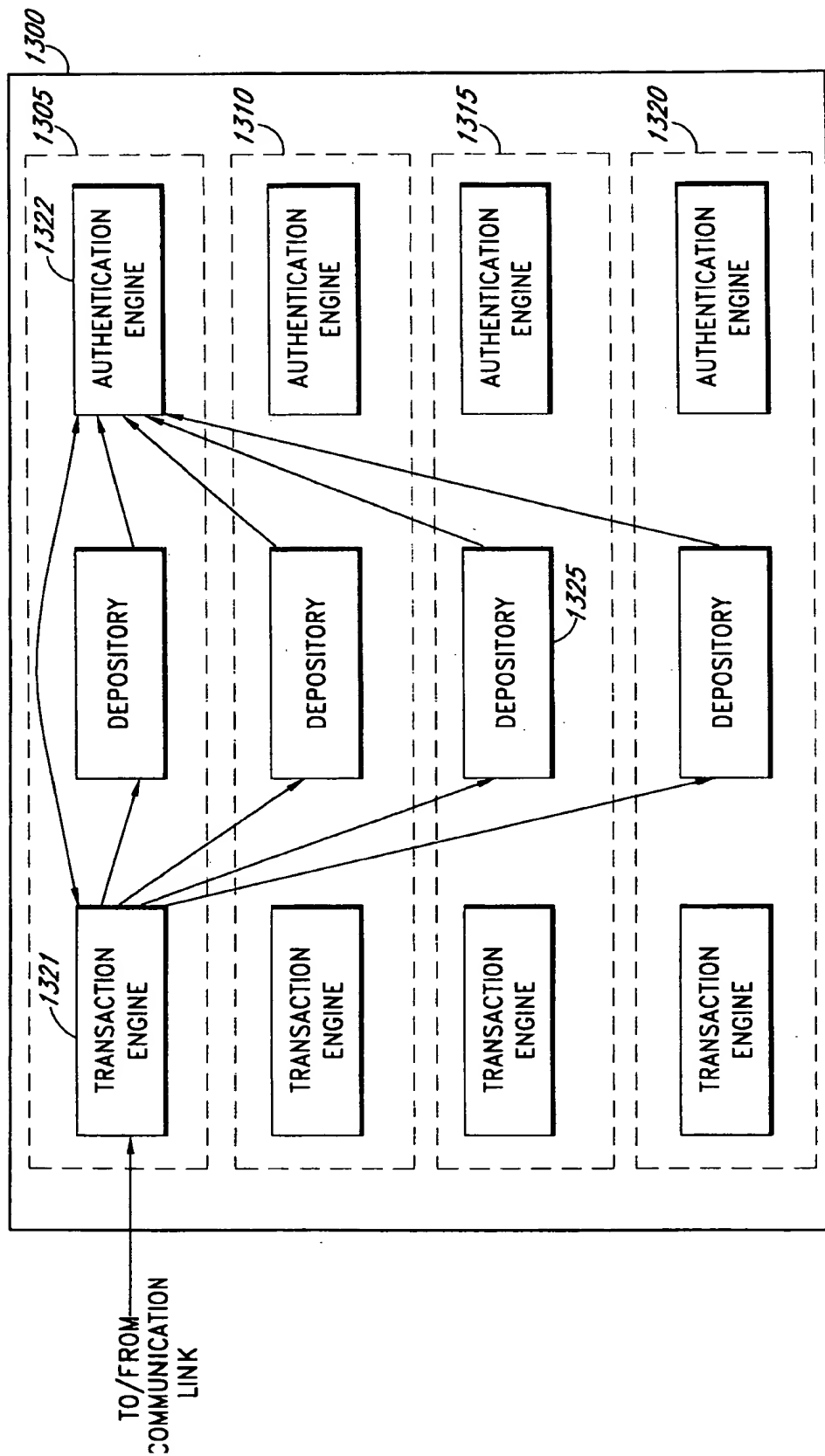
FIG. 10

| SIGNING DATA FLOW | | | |
|-------------------|---------------------------|------|--|
| SEND | RECEIVE | SSL | ACTION |
| USER | VENDOR | 1/2 | TRANSACTION OCCURS, SUCH AS AGREEING ON A DEAL |
| VENDOR | USER | 1/2 | TRANSMIT TRANSACTION IDENTIFICATION NUMBER (TID), AUTHENTICATION REQUEST (AR), AND AGREEMENT OR MESSAGE (M) |
| | | | CURRENT AUTHENTICATION DATA (B') AND A HASH OF THE MESSAGE RECEIVED BY THE USER (h(M')) IS GATHERED FROM USER |
| USER | TE | 1/2 | TRANSMIT TID, B', AR, AND h(M') WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS (PUB_AE(TID, B', h(M'))) |
| TE | AE | FULL | FORWARD TRANSMISSION |
| | | | GATHER ENROLLMENT AUTHENTICATION DATA |
| VENDOR | TRANSACTION ENGINE (TE) | FULL | TRANSMITS UID, TID, AR, AND A HASH OF THE MESSAGE (h(M)). |
| TE | MASS STORAGE (MS) | FULL | CREATE RECORD IN DATABASE |
| TE | THE Xth DEPOSITORY(DX) | FULL | UID, TID |
| DX | AE | FULL | TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX), AS (PUB_AE(TID, BX)) |
| | | | THE ORIGINAL VENDOR MESSAGE IS TRANSMITTED TO THE AE |
| TE | AE | FULL | TRANSMIT h(M) |
| | | | AE ASSEMBLES B, COMPARES TO B' AND COMPARES h(M) TO h(M') |
| AE | CRYPTOGRAPHIC ENGINE (CE) | FULL | REQUEST FOR DIGITAL SIGNATURE AND A MESSAGE TO BE SIGNED, FOR EXAMPLE, THE HASHED MESSAGE |
| AE | DX | FULL | TID, SIGNING UID |
| DX | CE | FULL | TRANSMIT THE PORTION OF THE CRYPTOGRAPHIC KEY CORRESPONDING TO THE SIGNING PARTY |
| | | | CE ASSEMBLES KEY AND SIGNS |
| CE | AE | FULL | TRANSMIT THE DIGITAL SIGNATURE (S) OF SIGNING PARTY |
| AE | TE | FULL | TID, THE FILLED IN AR, h(M), AND S |
| TE | VENDOR | FULL | TID, A RECEIPT=(TID, YES/NO, AND S), AND THE DIGITAL SIGNATURE OF THE TRUST ENGINE, FOR EXAMPLE, A HASH OF THE RECEIPT ENCRYPTED WITH THE TRUST ENGINE'S PRIVATE KEY (Priv_TE(h(RECEIPT))) |
| TE | USER | 1/2 | TID, CONFIRMATION MESSAGE |

FIG. 11

| ENCRYPTION/DECRYPTION DATA FLOW | | | |
|---------------------------------|--|------|---|
| SEND | RECEIVE | SSL | ACTION |
| DECRYPTION | | | |
| | | | PERFORM AUTHENTICATION DATA PROCESS 1000, INCLUDE THE SESSION KEY (SYNC) IN THE AR, WHERE THE SYNC HAS BEEN ENCRYPTED WITH THE PUBLIC KEY OF THE USER AS PUB_USER(SNYC) |
| | | | AUTHENTICATE THE USER |
| 1205 AE | CE | FULL | FORWARD PUB_USER(SYNC) TO CE |
| 1210 AE | DX | FULL | UID, TID |
| 1215 DX | CE | FULL | TRANSMIT THE TID AND THE PORTION OF THE PRIVATE KEY AS (PUB_AE(TID, KEY_USER)) |
| 1220 | CE ASSEMBLES THE CRYPTOGRAPHIC KEY AND DECRYPTS THE SYNC | | |
| 1225 CE | AE | FULL | TID, THE FILLED IN AR INCLUDING DECRYPTED SYNC |
| 1230 AE | TE | FULL | FORWARD TO TE |
| TE | REQUESTING APP/VENDOR | 1/2 | TID, YES/NO, SYNC |
| ENCRYPTION | | | |
| 1235 REQUESTING APP/VENDOR | TE | 1/2 | REQUEST FOR PUBLIC KEY OF USER |
| 1240 TE | MS | FULL | REQUEST DIGITAL CERTIFICATE |
| 1245 MS | TE | FULL | TRANSMIT DIGITAL CERTIFICATE |
| 1250 TE | REQUESTING APP/VENDOR | 1/2 | TRANSMIT DIGITAL CERTIFICATE |

FIG. 12

**FIG. 13**

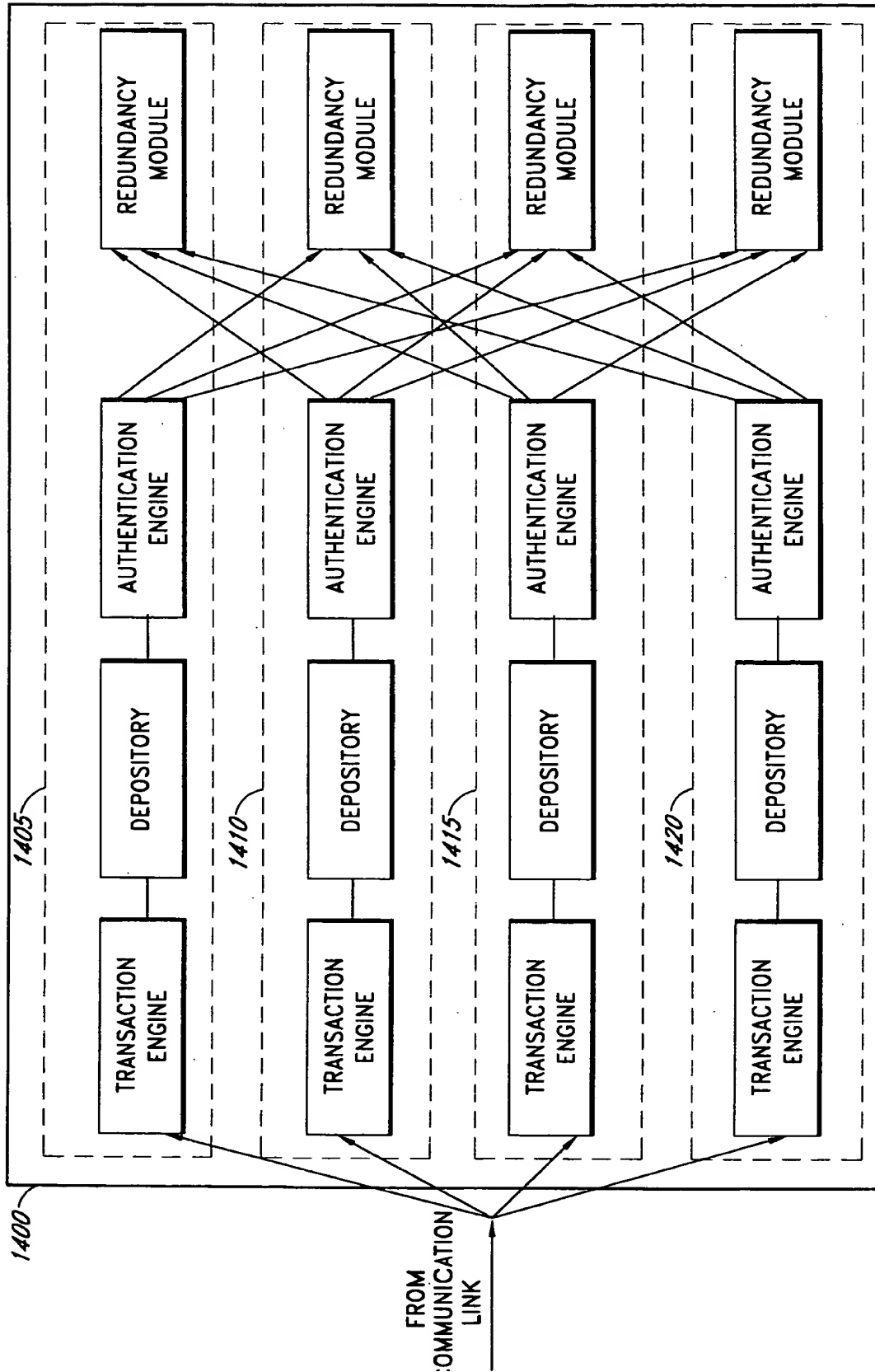


FIG. 14

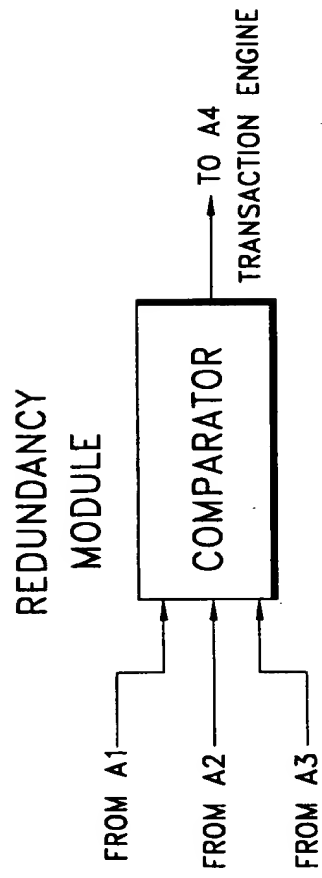
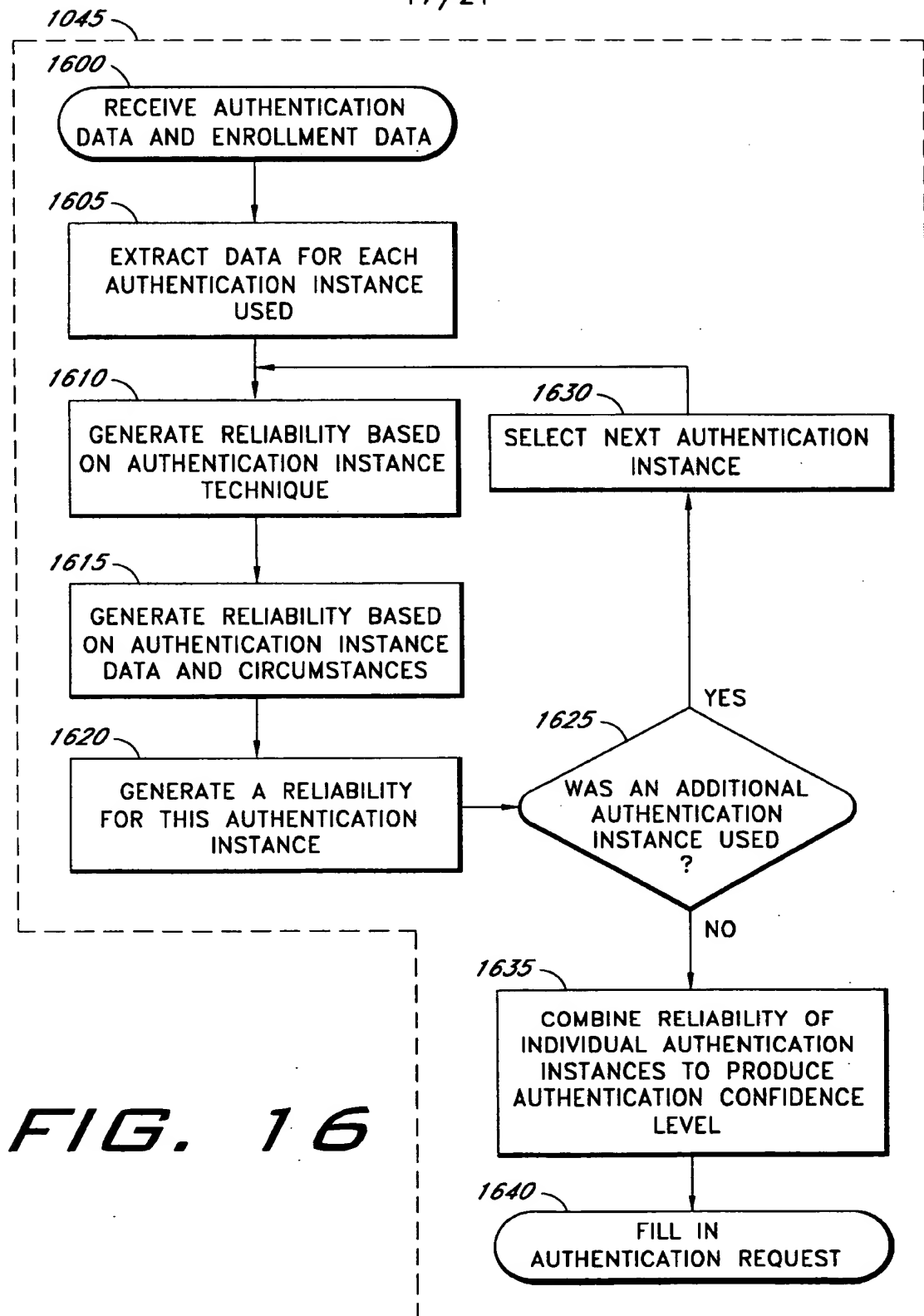
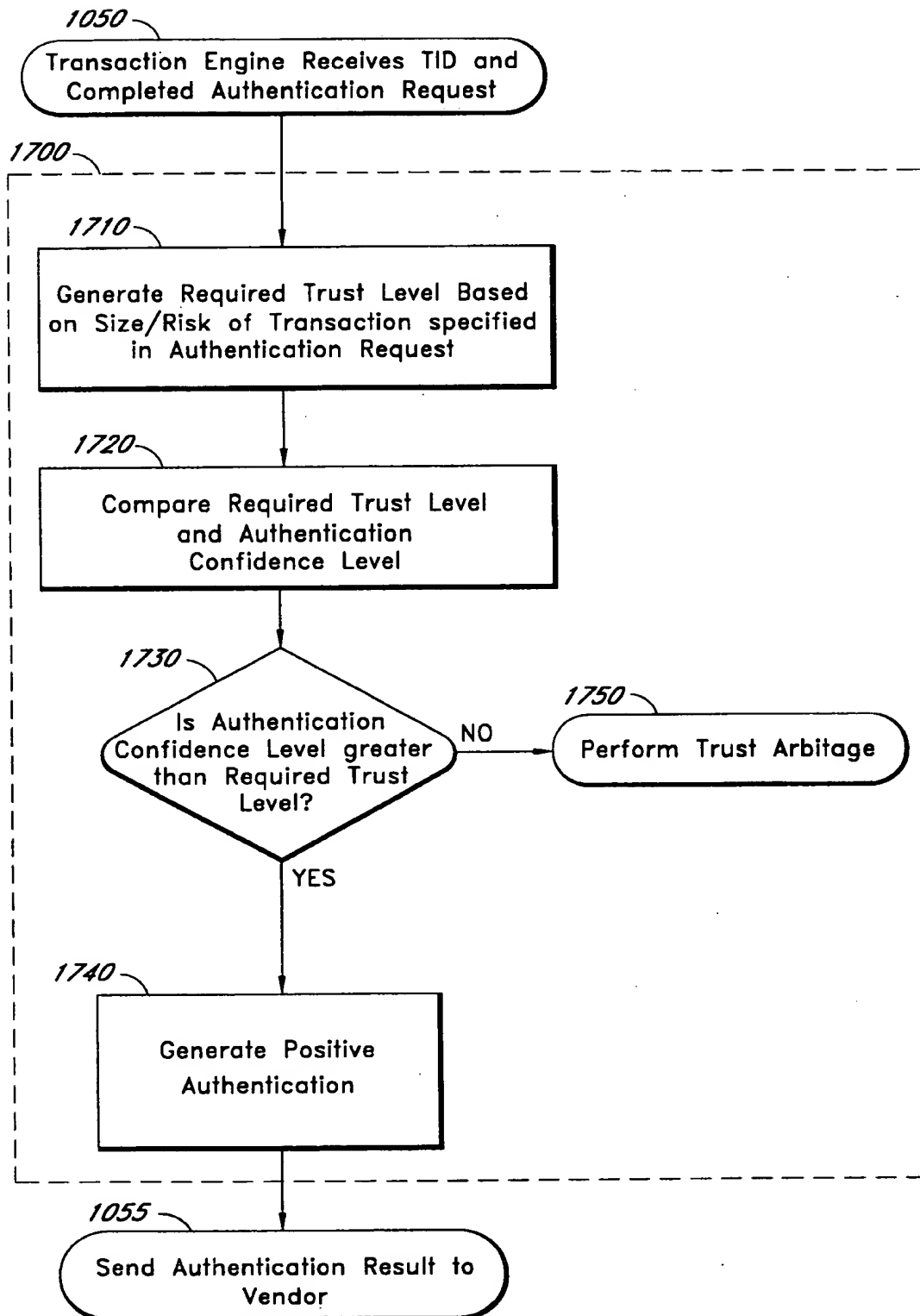
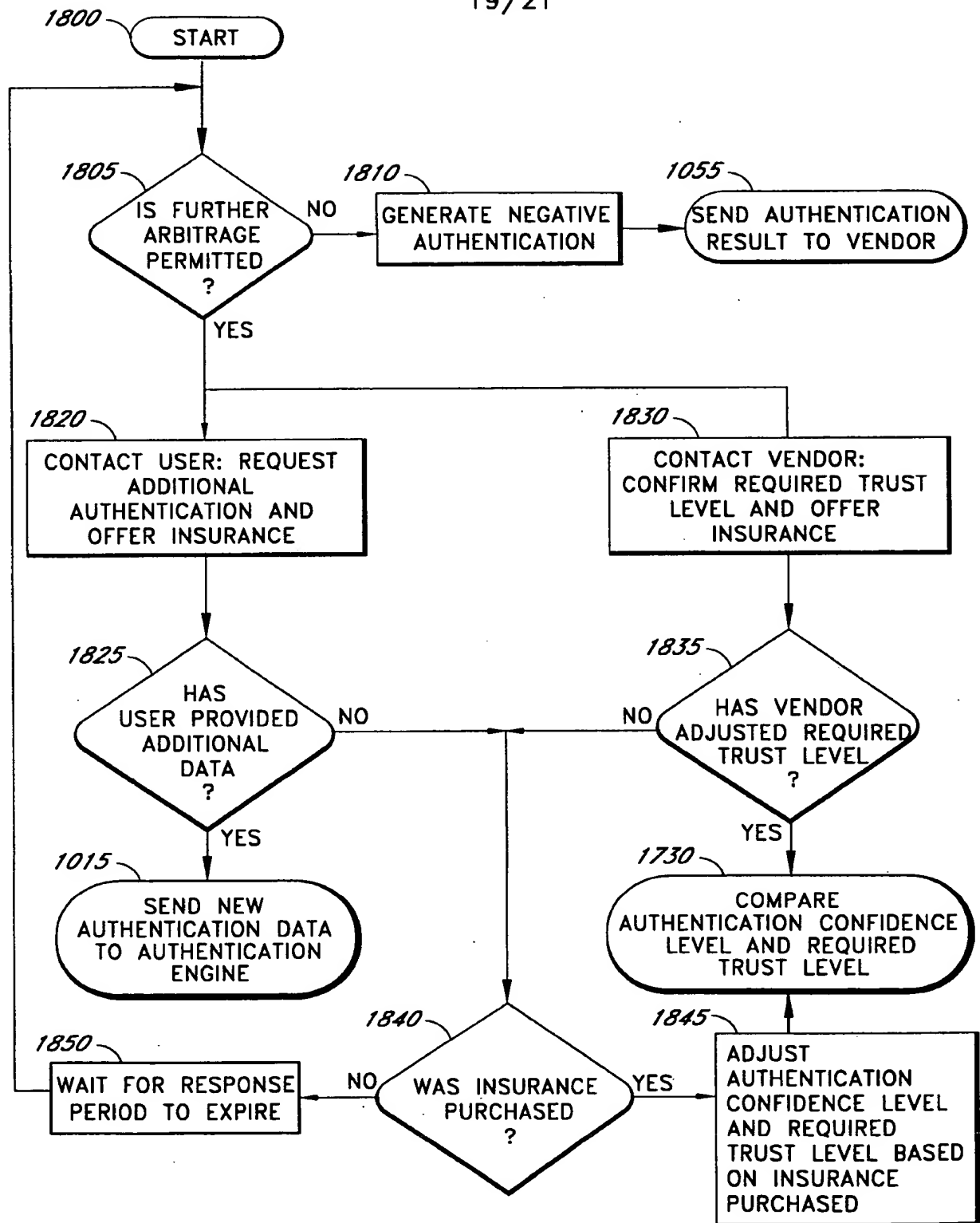


FIG. 15

**FIG. 16**

**FIG. 17**

**FIG. 18**

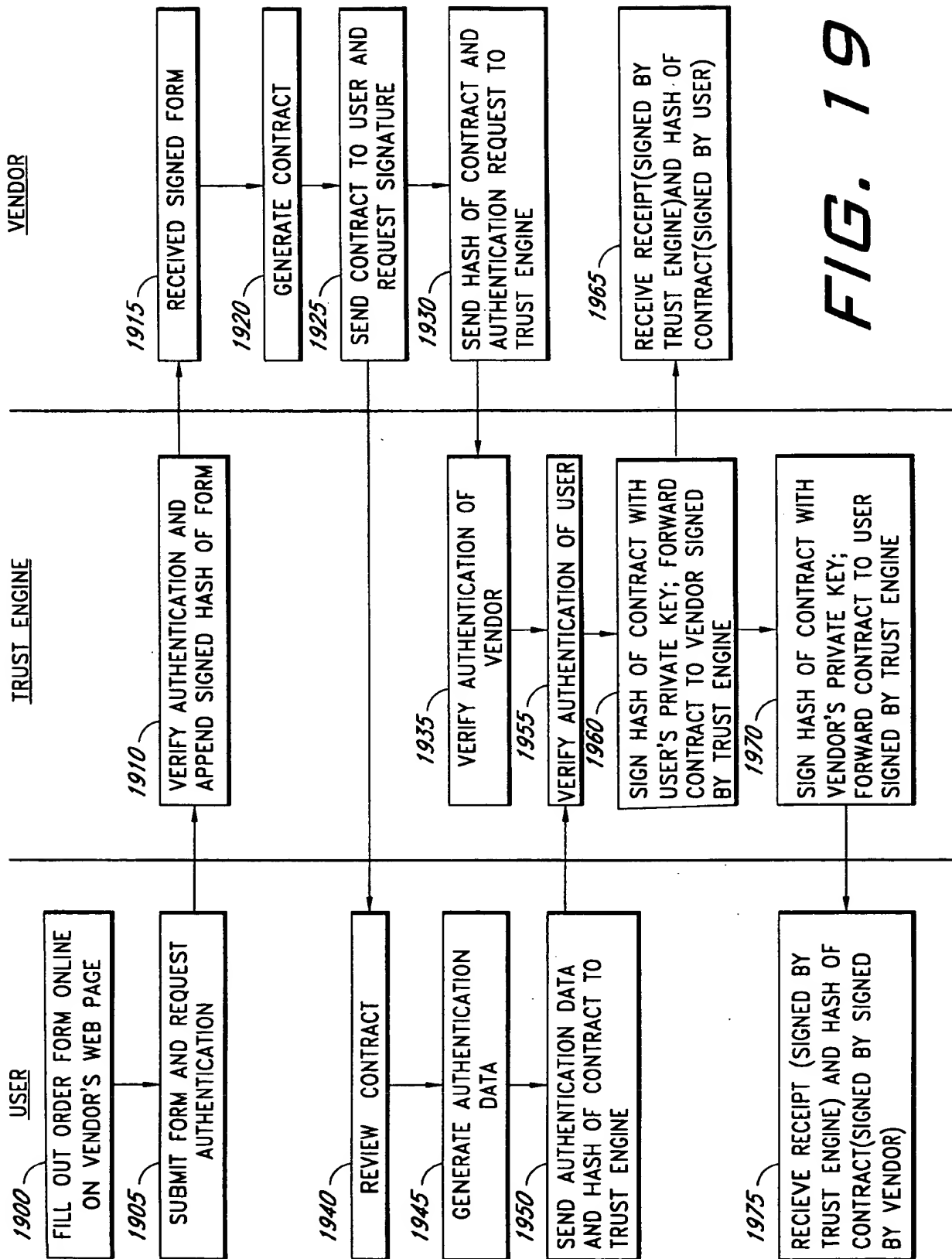
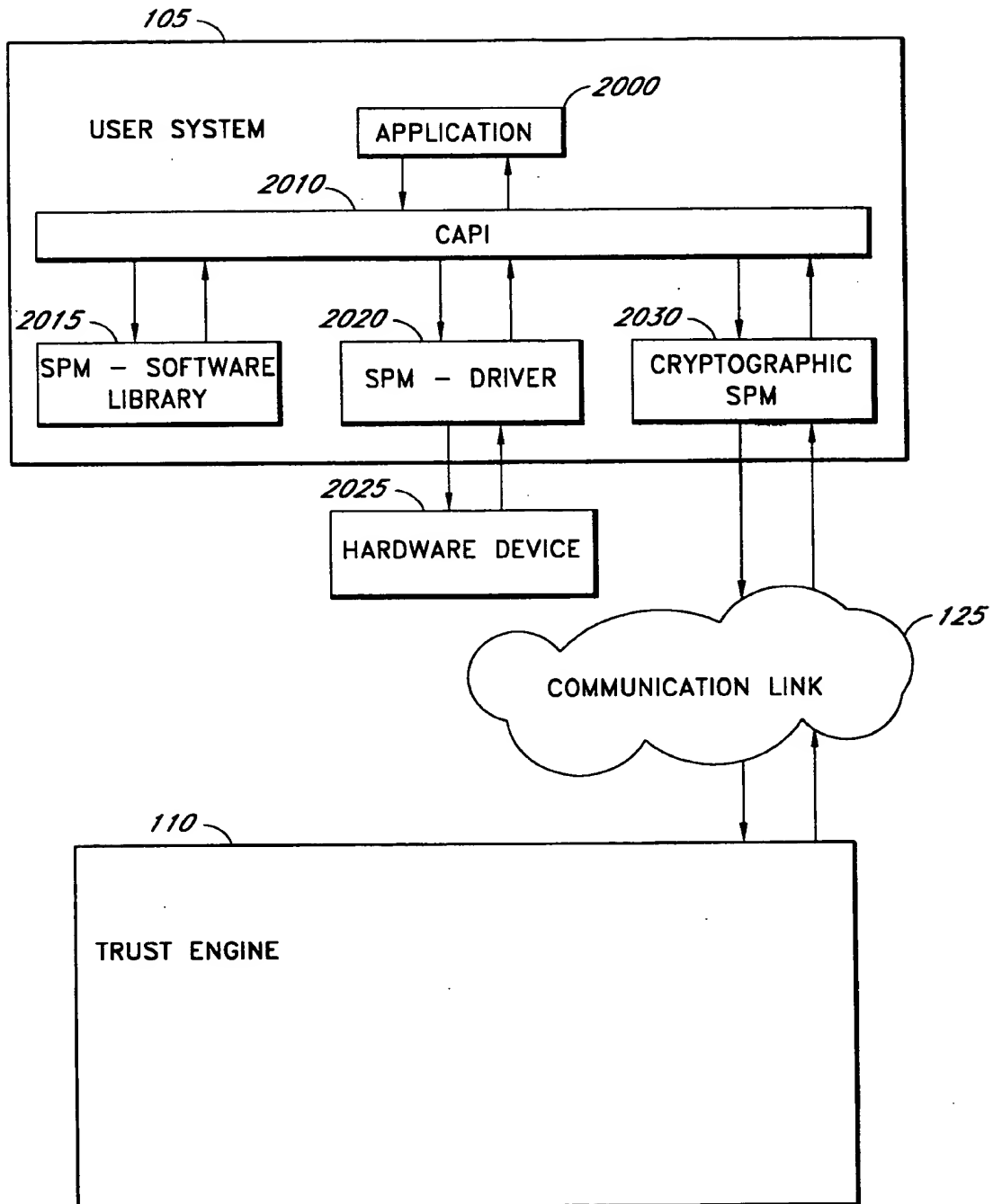


FIG. 19

**FIG. 20**